TERRI AGNEW: 6 de Abril del 2015 a las 23 horas UTC. Como éste es un seminario, no vamos a hacer la verificación de asistencia. Pero les recuerdo a todos los participantes que silencien sus micrófonos y sus computadoras. Y que también digan sus nombres al tomar la palabra, no sólo para la transcripción, sino para que nuestras intérpretes los identifiquen correctamente.

Contamos con interpretación al inglés y al portugués.

Muchas gracias.

Y ahora le doy la palabra a Silvina Vivanco, la moderadora de esta teleconferencia.

SILVINA VIVANCO: Gracias Terri. Silvia Vivanco, del personal de At-Large.

Les quiero dar la bienvenida al webinar DNS básico, el cual ha sido organizado conjuntamente con el equipo de ICANN de relacionamiento global GSE de Latinoamérica y el Caribe, LACRALO y el personal de At-Large.

Este es uno de los proyectos del plan estratégico de ICANN para Latinoamérica y el Caribe para este año 2015.

Este webinar tiene como objetivo proporcionarles conocimientos fundamentales para el cabal entendimiento de DNS, direcciones IP, nombres de dominio, registros de datos y el proceso de resolver dominios TLDs y gTLDs. Se abordará el tema de seguridad, estabilidad y resiliencia del DNS.

Me gustaría presentarle a mi colega en ICANN, Carlos Álvarez. Él es Gerente Senior de enlaces de Seguridad, Estabilidad y Resiliencia de la ICANN.

Carlos es abogado, examinador certificado de fraudes, y su trabajo se concentra en la colaboración basada en la confianza, con unidades de la ciberpolicía de países alrededor del mundo, y la comunidad internacional de seguridad operacional del sector privado.

Parte de sus funciones incluyen también dar entrenamiento a agencias de policías, administradores de gTLDs, y otros actores involucrados en la operación o la seguridad de los identificadores de internet.

Carlos les hablará también de la labor que desarrolla su Departamento, la cual es fundamental para la seguridad, la estabilidad y la resiliencia del DNS. Les explicará la labor de facilitación en el mantenimiento de seguridad y resiliencia.

Alberto Soto, seguidamente, les hará una presentación que consta en una explicación de lo que es registros de nombre de dominio, incluyendo ccTLDS y gTLDS. El proceso de resolución de nombres de dominio, cómo funciona el DNS, y nos dará un ejemplo y nos explicará qué sucede cuando queremos leer un diario de España, desde Argentina.

La metodología de este webinar. Primero tendremos todas las exposiciones, seguidas al final de preguntas y respuestas.

Les pedimos por favor que escriban sus preguntas en el chat del Adobe Connect, especificando a quién van dirigidas, o levanten la mano para preguntar. El Staff tomará las preguntas en orden de llegada.

Sin más comentarios, le doy la palabra a Carlos Álvarez. Adelante Carlos.

CARLOS ÁLVAREZ: Buenas tardes a todos, y gracias Silvia por la introducción.

No tenemos mucho tiempo, así que vamos directo al grano. Vamos con los cuatro temas que vamos a tocar entre Alberto y yo. Voy a hacer un esfuerzo por hablar suficientemente despacio para que los intérpretes puedan hacer su trabajo sin confusiones por mi defectuosa pronunciación. Pero suficientemente rápido para que abordemos todos los temas.

Los cuatro temas que vamos a tocar son inicialmente, identificadores únicos de internet, vamos a ver qué son, en qué consisten, para qué sirven. Alberto va a exponer acerca del registro de nombre de dominios, del proceso de resolución de nombres de dominio. Y finalmente, como Silvina indicó, les explicaré un poco qué hacemos en el Departamento de Seguridad, Estabilidad y Resiliencia.

Entonces, qué son los identificadores únicos de internet. Lo primero que encontramos es que todos los aparatos de hardware, todos los aparatos que son capaces de conectarse a una red, un computador, un teléfono, una impresora, una nevera, ahora con el internet, las cosas, las bombillas de luz, los teléfonos de escritorio. Todos tienen una dirección que está asociada a su cuerpo físico, al hardware como tal. Estas direcciones se conocen con el nombre de MAC adress, dirección MAC, simplemente.

Estas direcciones son únicas para cada aparato. Únicas en el sentido de que realmente, solamente un único aparato, en toda la historia, en todo

el planeta, puede tener esa dirección MAC. Únicamente en los casos de falsificación, que tristemente, se presentan, puede haber direcciones MAC que estén repetidas. El resto, en los casos en que la asignación de la dirección MAC, por parte del fabricante del hardware, ha sido hecha de manera legítima, las direcciones MAC van a ser únicas.

Ahora vamos a ver la relación que existe entre las direcciones MAC y el enrutamiento. Los primeros pasos del routing, en una red local, y de una red local a una red sobre protocolo de internet, que eso ya nos acerca un poco más hacia la necesidad de la existencia de los dominios, y de la resolución de los dominios, que les explicara Alberto adelante.

Vale aclarar, como verán en las diapositivas, las direcciones son MAC son series de caracteres hexadecimales. Son seis pares separados, valga la redundancia, por un separador consistente en dos puntos. Y en la siguiente diapositiva pueden encontrar unas instrucciones para encontrar la dirección MAC del aparato que ustedes utilizan, del Si usan una máquina Windows, pueden ejecutar CMD.exe, y cuando salga la pantallita negra, con el command prompt, que les pide más comandos, pueden escribir get MAC. Si están en un sistema operativo en Mac o en Linux, utilizan open vsd, que es la terminal que permite, al usuario, interactuar con la máquina, a través de comandos. Pueden escribir IF config y IS config, y en los resultados, buscan uno que inicie con la palabra either, y ahí encontrarán su dirección.

Igualmente, para los teléfonos IPhone y Android, ahí encuentran la ruta que deben seguir para encontrar la dirección MAC de sus dispositivos.

Usualmente no es muy relevante, no es muy relevante conocer la dirección MAC, porque los usuarios nunca se preguntan cómo funcionan

las máquinas, cómo funcionan los dispositivos, y por qué internet funciona. Pero si algún día tienen curiosidad, ahí está la información.

Con la dirección MAC, un dispositivo o una máquina, puede comunicarse con los demás dispositivos, con las demás máquinas, o computadores, que estén en su red local. Pero no puede salir de internet.

Para poder salir de internet, y con esto me refiero a conectarse a un router, y que el router pueda, perdonen la redundancia, enrutar la comunicación hacia afuera, hacia el internet como tal. El dispositivo que se quiere conectar debe recibir una dirección bajo el protocolo de internet, o sea una dirección IP. Las direcciones IP de las que con certeza han oído algo, existen dos clases. Existe la versión 4, existe la versión 6. Sin entrar en muchos detalles, aquí ven un ejemplo de una dirección en la versión cuatro, que es 192.168.2.1.

Generalmente, no existen personas que tengan la capacidad de recordar direcciones IP bajo la versión cuatro, menos aún bajo la versión seis, bajo IPv6. En el texto en rojo al final de la diapositiva es una dirección IP bajo la versión seis. Son caracteres hexadecimales largos, que muy difícilmente alguien podría recordar. Y esas direcciones IP son necesarias para que el enrutamiento de las comunicaciones entre las máquinas se pueda dar.

Esta fue la razón por la que, hace varias décadas, los padres de internet tuvieron la idea de crear el sistema de nombres de dominio, porque crea identificadores que son humanamente recordables, fácilmente recordables, que se asocian a direcciones IP. Nos quitaron un problema de encima. Es más fácil recordar ICANN.org a recordar una cantidad de

direcciones IP que pueden ser usadas para correo electrónico, para servidores FTP, para servidores web, en fin.

Como decía ahora, los dispositivos deben conectarse al router, un nombre, en términos de enrutamiento que se le da a los router, es gateway, es la puerta a través de la que la máquina sale de su red de área local hacia el internet.

Lastimosamente, en Adobe Connect, la sala de reuniones en la que estamos en este momento, no deja ver un dialogo que se da entre ese portátil y el router que ven ahí. El portátil envía un mensaje hacia toda la red interna en la que ella está, la red de área local, preguntando "¿Alguien puede ayudarme a conectarme a una red? quiero salir a internet", y el router le responde "Bienvenido, yo le puedo ayudar, soy su gateway. Mi dirección es 192.168.4.1" es un ejemplo.

Su dirección IP es tal, 192.168.4.1. Nuestra máscara de subred es 255.255.252.0. Son ejemplos.

Cuando el router, o el gateway, le asignan una dirección IP a la máquina, ya puede haber salida de las comunicaciones hacia el internet exterior. Es impreciso decirlo así, pero digamos que ya puede haber comunicación bajo el protocolo de internet.

Ahí está el dialogo entre el portátil y el router. Entonces el portátil envía la pregunta "¿Alguien puede ayudarme a conectarme a una red?", llega la red, y el router le responde "yo soy su gateway, mi dirección es tal, su dirección IP es tal, y la subred en la que estamos es la siguiente".

No voy a entrar en detalle de qué es la subred. Solo mencionarlo a grandes rasgos. Por decirlo de una manera de corta, es el nombre de la red local, o el número que identifica a la red local.

Y ahí el computador recibe esa información, y ella con eso puede hacer entonces el proceso de enrutamiento de los datos.

Ahora, para asociar las dos direcciones, la dirección MAC y la dirección IP, debe existir algo que le permita a la máquina que le permita trabajar con ambas, porque él tiene, en el hardware, una dirección MAC, qué está, como se dice en inglés, en hard coded, es una dirección que le pertenece al hardware.

Pero la dirección IP está en otro nivel, está en un nivel que no está asociado al hardware, y la máquina tiene que poder conectar el nivel de hardware y el nivel de la dirección IP.

Entra en juego un protocolo que se llama el Adress Resolution Protocol, o ARP. El protocolo ARP, justamente, asocia las direcciones MAC con las direcciones IP en la red de área local.

Aquí está mencionado un ejemplo, en el que ustedes pueden ver que al utilizar el comando ARP-A, en una máquina Mac, pueden encontrar las direcciones IP, que han sido asociadas a máquinas en la misma red local, y las correspondientes direcciones MAC de sus dispositivos.

Así, ya mi computador ya va a saber si tiene que comunicarse con otro computador, con un servidor, ya va a saber cuál es la dirección IP de esa máquina, y cuál es la dirección MAC de ese dispositivo.

Hay un tema que es muy interesante, lo voy a mencionar brevemente y ya dejo paso a Alberto, para que respetemos el tiempo, en lo posible.

Existen varias clases de direcciones IP. A grandes rasgos, y por simplificar en efectos de la presentación, digamos que existen dos grandes clases, las direcciones privadas y las direcciones públicas. Las direcciones privadas son direcciones que solamente pueden existir, o deben existir en redes internes. Si ustedes se fijan en el slide debajo de la flecha azul, dice ver RSC3330. Eso dice IP adress, y hay un link.

Si ustedes hacen clic en ese link, van a llegar a un estándar de internet, que fue definido por la IETS, que es la fuerza de trabajo sobre la ingeniería de internet. No sé si es la traducción oficial. Es la Internet Engineering Taskforce. Es el estándar que define cual es el uso que se le puede dar, usos especiales, que se dan en algunos bloques de direcciones IP. Y ahí encuentran los rangos. De tal número a tal número, son direcciones que van a ser utilizadas para este fin, de tal número a tal número, las direcciones deben ser utilizadas con éste otro fin.

Entonces, en general, cuando yo me conecto a internet, mi ISP me asigna una dirección que está, ISP entendido obviamente, para clarificar, como el proveedor de servicios de internet, una empresa que yo contrato, a la que le pago un mensual, que me ofrece el servicio de internet. El ISP debe asignarle a mi computador, o a mi aparato, una dirección que esté en el rango de las correspondientes a las direcciones públicas.

Sin embargo, hay una práctica que no es muy apreciada, que no es muy bien recibida. Algunos ISP asignan direcciones dentro de los rangos que

corresponden a direcciones privadas. Eso se conoce en inglés como carrier grade NAT, o CDN. NAT quiere decir Network Adress Translation.

O sea, lo que hace el servidor del ISP es que, en lugar de considerar que todos sus clientes, todas las máquinas son parte de internet, lo que hace es que ponen una barrera grande y divide el tráfico que está hacia afuera del ISP es internet, y el tráfico que está adentro del ISP, es decir sus clientes, en realidad no están en internet, están en una red de área local, que puede ser muy grande. Puede ser un barrio, pueden ser varios barrios, varias vecindades, depende de la configuración o del alcance geográfico del ISP.

Y por qué esta práctica del carrier grade NAT no es muy apreciada, esa no es una palabra exacta, por qué no nos gusta mucho, por decirlo así, a algunos que tratamos de mantener el internet un poco más seguro y más amigable, para que nuestros niños y nuestras familias puedan estar en internet de una forma un poco más tranquila. Es porque dificulta la labor de identificación de las personas que hacen cosas malas en internet.

La anonimización en internet, es muy relativa. Los que dicen que por utilizar la red TOR, que es un sistema, un servicio, que permite anonimizar el tráfico, o los que creen que pueden hacer cosas sin ser encontrados en internet, están muy equivocados.

Siempre es posible en últimas, con mayor o menor dificultad, encontrar a quien ha hecho algo. Este carrier grade NAT dificulta, porque ya depende de que el ISP guarde los registros de a quien le asigno la dirección de IP interna, dentro de su red de área local que corresponde a sus clientes.

No me voy a extender más en esto. Si alguien tiene sobre esto una pregunta, con gusto lo podemos ver al final, o por escrito, con todo gusto.

Ahora si nos [inaudible], el inicio de la siguiente diapositiva, que le corresponde a Alberto. Adelante Alberto.

ALBERTO SOTO: Gracias. Alberto Soto.

Muy amable Carlos, saludo nuevamente a todos. Buenas tardes, buenas noches, buenos días, a los que han entrado después que yo.

Cuando estuvimos charlando un poco con Carlos a ver qué pasaba con lo que íbamos a decir, descubrimos que los dos somos abogados. Y dos abogados hablando de cosas técnicas, dijimos qué va a salir de aquí. Pero bueno, parece que algo está saliendo hasta ahora. Por lo menos hasta que estoy entrando yo.

Carlos ya ha dicho sobre las direcciones IP. Qué pasa cuando, si todos deberíamos recordar, como dijo, los numeritos para un diario, para un servicio, para entrar a Facebook, para entrar a cualquier sitio web, sería imposible. Entonces, para eso, existe lo que se llama el DNS, que normalmente los técnicos van a decir qué es un DNS. Es un servidor, es una computadora, que resuelve los nombres de dominio. Pero DNS, en realidad, dentro de nuestra ICANN, es un sistema, es todo un sistema, que resuelve los nombres de dominio, y que hay, como vamos a ver dentro de un ratito, un montón de computadoras que pueden llegar a resolver este tema.

Por favor, adelante Terri.

Para que comprendan, exactamente, voy a tratar de hablar claro. Si alguien ve esto, dígame si lo entiende o si no lo entiende. ¿Alguien levanta la mano? Todo el mundo lo entiende. Bueno, pasamos a la otra, por favor Terri.

Bueno, esta es un poco más simple. ¿Alguien lo entiende? Si alguien lo entiende, por favor no me lo diga, dígame alguien que no entiende, porque ya sé que hay gente que entiende esto. Nadie entiende esto. Bueno, lo dejamos. Adelante Terri, después volvemos.

Bien, como dije, Domain Name System, DNS, es el sistema. Vamos a analizar ahora. Como en varios idiomas, vamos a empezar a escribir al revés, no como estamos acostumbrados a escribir. Por ejemplo, United Kingdom, UK, .ORG, .yourdomain, .www. ¿Qué es United Kingdom? United Kindom, recuerdan los problemas que tuvimos con .patagonia, no, ese no. Otros problemas que tuvimos con dominios de dos letras, se dio mucho porque, normalmente las dos letras se utilizan para el código de país, que para que ICANN es el crossed country top level domain, ¿recuerdan ahora?

Es decir, junto con el otro, el .com, .org, y todos los demás similares a esto, son lo que se denomina, dentro de ICANN, top level domain, o sea dominios de alto nivel.

El de dos letras, que identifica a los países, como todos conocemos, hay un grupo que está trabajando sobre el crossed country top level domain. También hay otro que está trabajando sobre el generic top level domain.

Es decir, con eso ya estamos viendo que dentro de ICANN, todas las políticas de nombre de dominio están siendo tratadas específicamente por alguien.

Perdón Carlos, tienen razon, es country code top level domain, no crossed country. Si lo quieren corregir, por favor.

Luego tenemos, en este caso del ejemplo, your domain, ¿qué es? Es el representativo de una persona de una organización, o de una empresa. Con esto, vamos a tener lo que se llama el nombre de dominio. Es decir, yourdomain.org.uk. Y recuerden esto, porque va a ser una de las preguntas de las trivias seguro. "¿Cómo se representa un nombre de dominio?", o algo parecido.

La URL es la dirección completa que yo tengo que escribir, para poder llegar a un sitio web cualquiera.

Adelante Terri por favor.

Entonces, dije que si yo le pregunto a un técnico qué es un DNS, me va a decir que es un computador que resuelve nombres de dominio. Para nosotros, para nuestra concepción, tenemos que ver que es todo un sistema que tiene ICANN, y es el principal que tiene, por supuesto, que hace simplemente la traducción del nombre de dominio, que es una dirección alfanumérica. ¿Por qué alfanumérica?, porque los nombres de dominio pueden tener caracteres numéricos, aparte de alfabéticos, hay unos cuantos que los tienen.

Transforma ese nombre de dominio, que es una dirección alfanumérica, en una dirección numérica, que es la dirección IP que acaba de explicar Carlos, y viceversa. ¿Por qué viceversa?, porque cuando yo escribo

traduce, va a buscar la ubicación de ese site que yo quiero ver, y luego me la devuelve. Es decir, este, cuando se completó ese camino, me resolvió el nombre de dominio, mi sistema de nombre de dominio, el Domain Name System, me resolvió el nombre de dominio que yo escribí.

Adelante, por favor, Terri.

El proceso, cómo resuelve el DNS. Cuando yo consulto una página cualquiera, cuando escribo en un navegador, como dijo Carlos, va a haber un router, un equipo, es otra computadora, que cumple la función de, como su nombre lo dice, enroutar, ir a un determinado lugar. En este caso, internet tiene la forma de un árbol invertido. Entonces, si no encuentra lo que yo le pido que busque, en la primer instancia, la va a buscar en otra, y en otra, y así sucesivamente, hasta encontrar lo que se llama un servidor de nombre raíz, que hay trece, que son los principales del DNS.

Nunca va a llegar a los nombres raíces o búsqueda, ahora vamos a ver por qué. Porque hay servidores de nombre de dominio, que resuelve mucho antes que llegue a este caso. Esto sería muy hipotético, que no pueda resolverse un nombre de dominio, y que haga llegar al servidor raíz. De hecho, prácticamente se tocan poco los servidores raíz.

Como dije antes, todo parte de las letras. Convierte a números, y así resuelve el nombre de dominio.

¿Por qué normalmente no hay problemas?, porque existe un servidor DNS primario, en mi proveedor de servicio, y también un servidor DNS secundario. ¿Qué son estos?, son computadores que sirven para

resolver rápidamente, y que yo no tenga que viajar tanto por el ciberespacio para buscar la resolución del nombre de dominio que estoy buscando.

Yo estuve en una empresa, era una empresa de desarrollo de soft, y teníamos un data center, y teníamos nuestros propios servidores de dominio, primario y secundario. Es decir, ya hay cosas tan redundantes, que sirven para mejorar, para que no pase como pasaba antes.
Ahora voy a decir qué pasaba antes.

Luego que la información, esa que yo pedí, es obtenida, va a llegar hasta mi dispositivo, del cual hice la consulta, y podré acceder a la página web solicitada.

¿Hola?

Sigo entonces. ¿Hola?

SILVIA VIVANCO: Adelante, se escucha.

ALBERTO SOTO: Perdón, parecía que se me había cortado.

Entonces, yo dije, de un dispositivo, del dispositivo que yo hice la consulta del sitio web, pero recuerden, yo no estaba leyendo, pero arriba en el tercer punto dice "si no encuentra la información en su computadora, teléfono, Tablet, PlayStation, reloj inteligente, heladera, etcétera, etcétera". ¿Por qué digo esto?, porque ya hay hasta heladeras que, cuando yo saco una botella, va cargando en sus sistema que tiene

una botella menos de lo que yo saqué. Y va cargando. Y en un momento determinado, según sea programada, va a hacer una llamada al supermercado, y va a hacer el pedido correspondiente de lo que yo haya sacado en dos días, o en un día, según sea la programación.

Esas serian direcciones IP internas, de las que hablaba Carlos. Pero la cantidad de comunicaciones que están pidiendo, resolución de nombre de dominio desde muchísimos lugares. Adelante Terri.

Como yo decía, hace algunos años, muchos años, cuando yo hacía una consulta, escribía una URL, recuerden URL es Uniformed Resource Location, en español sería Localizador Uniforme de Recursos. En ese momento, cuando se iniciaba internet, no había un servidor de nombre de dominio que resolviera, en Buenos Aires, en Argentina, se resolvía en Estados Unidos.

Tiempo después, pusieron una réplica de un servidor raíz en Argentina, y eso mejoró muchísimo. Luego, fue avanzando el tiempo, y la organización, que era la cámara Argentina de Internet, allí estaba ese servidor réplica, replicó a su vez, puso servidores DNS en las distintas regiones de Argentina, y así, localmente, quien quería resolver un nombre de dominio, lo tenía mucho más rápidamente que ir hasta Estados Unidos y volver, o ir hasta Buenos Aires, y volver. Si estaba en Córdoba, iba hasta donde estaba el DNS de Córdoba, y volvía.

Y ahora, los proveedores de servicio de internet de cada lugar, tienen sus propios DNS. Eso fue mejorando bastante la performance en internet.

Antes yo daba un enter, iba a tomar un café y volvía, y esperaba. Y ahora, todavía no, pero llegaron Facebook, Twitter, y todas las redes sociales que vuelven a congestionar, y hacen que el ancho de banda que yo tenga, que antes era de 48k, ahora con 10 megas no me alcanza tampoco.

Adelante, por favor, Terri.

Ésta es una lista de los root servers. Como yo dije, fíjense que hay distintas organizaciones, de distinto orden, por ejemplo, saben quién es VeriSign, VeriSign es quien vende el .com, hay universidad, el tercero Cogent Communications es, aparte de que está manteniendo un servidor raíz, es un importante carrier de comunicaciones. Otra universidad, la nasa, ICANN tiene uno solo, RIPE, de Estados Unidos, y así sucesivamente.

Es decir, estos servidores raíces tienen, no vamos a entrar en ese detalle ahora, pero tienen letras, y están replicados en muchas partes del mundo. Recuerdo que debe haber, Carlos, si me equivoco, entre cuatrocientos cincuenta y quinientos DNS replicados.

CARLOS ÁLVARES: Perdón Alberto, ¿Puedes repetir la pregunta?

ALBERTO SOTO: Si, creo que, si no me equivoco, debe haber entre cuatrocientos cincuenta y quinientos DNS replicados, desde los servidores raíz.

CARLOS ÁLVARES: Voy a utilizar tu pregunta para complementar algo que dijiste anteriormente, y a medida que lo complemento, te respondo, si te parece.

ALBERTO SOTO: Adelante.

CARLOS ÁLVARES: El DNS, como sistema, es una base de datos distribuida, que no es operada por ICANN, sino que es operada por muchas organizaciones en muchos países. El root, como tal, es operado por VeriSign. VeriSign mantiene el root en servidores con niveles de seguridad muy altos. Las réplicas de los servidores raíz son administradas por las entidades que están listadas en el slide que nos está mostrando Alberto.

De ahí para abajo, el sistema se distribuye granularmente, de una manera que lo hace resiliente, que lo hace estable y que lo hace poco probable de sufrir caídas o interrupciones.

Ahora cuando me detuve un momento a pensar, tuve en mi cabeza al tiempo, dos procesos que son similares pero diferentes, que son uno la resolución de los dominios, y otro es el registro de los dominios cuando llega a los administradores de los dominios de alto nivel. Por eso frené un segundo, porque tuve que aclarar en mi cabeza esos dos conceptos.

En cuanto al proceso de resolución y a la replicación de, por un lado, los servidores raíz, y por otro, los servidores recursivos, los servidores raíz, que van de la A la M, cada servidor es un racimo de máquinas, no es una sola máquina, son muchas, muchas, muchas máquinas que están

distribuidas geográficamente. En el servidor L, por ejemplo, que opera ICANN, hay un concepto muy interesante que se conoce como root in the box, o sea, la raíz en una caja, y básicamente es eso, es una réplica del servidor L, que es una caja, una pieza de hardware pequeño, que se puede instalar sin un costo muy alto, tiene un costo bajo de instalación y administración, y eso permite que haya más resiliencia, que haya mejor manejo de la carga de consultas que llegan a los servidores.

Y un punto importante es que en la operación de los servidores raíz, se utiliza un protocolo que se conoce como any cast. El protocolo any cast hace que los servidores están asociados a, cada uno a un grupo de direcciones IP, pero dentro de los racimos de máquinas que corresponden a cada uno de los servidores de la A la M, cualquier máquina que este asociada a una dirección IP, va a poder responder a una consulta que llegue a esa dirección IP.

Esto tal vez no fue muy claro, y lo tengo presente. Normalmente, una dirección IP es un identificador único. Eso quiere decir que a una dirección IP corresponde una única máquina. Estoy hablando de direcciones IP públicas. En el caso de los servidores raíz, una dirección IP puede corresponder a muchas máquinas, y la razón es cercanía geográfica que disminuye el tiempo de tráfico de los paquetes de datos viajando entre servidores y clientes, y mayor resiliencia, de poder ofrecer mayor ancho de banda, menor tiempo de respuesta.

Y, un nivel abajo de los servidores raíz, se encuentran los servidores recursivos, y entramos a hablar de servidores autoritarios, que son los que, por ejemplo, VeriSign opera un servidor autoritario para los .com, PIR, que es Public Intrest Registry, opera el servidor autoritario para

el .org. Autoritario quiere decir que la información que su servidor provee es la información que es, y no se puede discutir. Es la que es. Es la verdad.

Debajo de esos servidores hay servidores que son recursivos, que lo que hacen es preguntar, y preguntar, y preguntar, a través de toda la cadena de servidores en el DNS.

Van hasta el root, después bajan hasta el servidor autoritario del .com, después van hasta el servidor autoritario de segundo nivel. Y se llaman recursivos, porque preguntan, reciben respuesta, vuelve a preguntar al siguiente, recibe respuesta, y cuando tiene la respuesta completa, se la envía a la máquina del usuario que quiere visitar www.icann.org.

Esos servidores recursivos que mencioné, que están por debajo de los autoritarios, tengo la certeza que se sabe cuántos existen, pero yo no tengo el número, y no sé qué tan actualizado les sea, que tan fácilmente actualizado le sea ese número, porque cualquier persona puede instalar un servidor de DNS que resuelva, que eso nos llevaría a otro tema, que ese es el de los resolutores abiertos, que es una preocupación muy grande, pero ese es otro asunto diferente.

Adelante Alberto.

ALBERTO SOTO: Gracias Carlos.

Y cuando Carlos dice que se podía instalar rápidamente y de forma segura, la tecnología hizo posible eso, porque antes, para poner un servidor con seguridad, necesitábamos una estructura, dentro del data

center, era sumamente importante para darle realmente la seguridad que requiere este tipo de equipamiento. La tecnología avanzó bastante, y abarató bastante los costos.

Vamos a ver los registros de nombre de dominio. Adelante Terri, por favor.

Como ya había dicho, los dominios podían estar conformados por letras y números. También es válido, por ejemplo, el guion, en tanto y en cuánto no esté colocado, ni al principio, ni al final del dominio.

Si, los dominios no pueden contener estos caracteres especiales, como puntos. Adelante Terri, por favor.

Entonces, hablamos que los dominios si tienen que registrarse. ¿Qué es el registro?, como dijo Carlos, es la base central donde se almacenan todos los nombres de dominios. A estas bases de datos, tienen acceso los denominados registradores. ¿Qué son los registradores?, un registrador es una organización que tiene acceso al registro, y por tanto, lleva a cabo el registro de los nombres de dominio. Y tiene que estar acreditada ante ICANN por un proceso que no vamos a ver ahora. Les dejé un link para, quién tenga interés, lo vea. Pero tienen que cumplir determinados requisitos, y recién pueden quedar autorizados para trabajar como registrador.

¿Y quién es registrante?, es la persona que compra un nombre de dominio, y de aquí en más, es el propietario del nombre de dominio, porque lo ha comprado. El registrador lo introduce, y una vez que lo introduce, va a comenzar a funcionar.

Adelante Terri, por favor. Voy a apurar así le dejo tiempo a Carlos.

Hay un sitio, que es internet.net, que es operado por ICANN, y ofrece información general sobre los registros de nombre de dominio. Allí podemos encontrar una lista alfabética de los registradores, o por ubicación, o por los idiomas que están admitidos.

Además, hay una tabla de ICANN con todos los registradores, y sus ubicaciones. Allí también está el link.

Pero como proceso de registro, ustedes pueden comprar a VeriSign directamente, a Go Daddy también, pero también a un proveedor acá en la Argentina, que es un intermediario. Y quiero aclarar esto, que si lo buscan adentro de ICANN, no lo van a encontrar, porque es un revendedor que tiene un arreglo comercial con un registrador, y que no tiene ningún tipo de relación con ICANN. Por lo tanto, ICANN lo desconoce totalmente, por no tener ninguna relación contractual con ellos.

Adelante Terri, por favor.

Ahora si vamos a leer el diario desde... Creo que algo han entendido de cómo se resuelve el nombre de dominio. En este caso, en el ejemplo que voy a dar, del país, ya está resuelto. El tracer es un comando que utilizan los técnicos para resolver determinados problemas, pero me sirve bien a mí para mostrar lo que quiero mostrarles.

Cuando yo escribo www.elpais.es, y doy enter, inmediatamente me aparece el renglón que está ahí. Y hay una dirección IP. Y esa dirección ya es la dirección del website elpais.es. Es decir, la resolución del nombre de dominio fue inmediata, absolutamente inmediata.

Luego, ahí dice, no lean todo, sino Telecentro. ¿Qué es Telecentro?, es mi proveedor de servicio, o su proveedor de servicio. El siguiente paso, y lo que va tardando ahí, si 14 milisegundos o 9 milisegundos, si es buena o mala performance, eso lo analizan los técnicos, pero es lo que está tardando.

Global crossing Argentina es la salida, es el proveedor, el carrier, el que da el ancho de banda más grande de salida del país, es uno de los carrier del país, y Telecentro se sirve de Global Crossing.

El renglón siguiente es F1, F1 es Ezeiza. Esa es directamente la salida desde Argentina. AR6 es un punto, que no sé dónde está, pero fíjense que salta a Los Angeles, Los Angeles, Palo Alto, New York, etc. Sigue a [Inaudible] 23.67.250.136, la tasa está completa. ¿Por dónde estuve navegando?, estuve navegando por la fibra óptica del Pacífico, que sale por Argentina, pasa por chile, va al Pacífico, y entra por Los Angeles, va a Palo Alto, de allí a Nueva York, y de allí salté creo que a la fibra óptica que va desde Estados Unidos a Europa, y la traza es completa.

La otra, por favor, Terri.

Aquí lo mismo, pero en Francia. Insisto en algo, la resolución del nombre de dominio fue absurdamente inmediata. Luego Telecentro sigue por Argentina, desde Global Crossing saltó a otro punto, y de allí a Miami, y en ese caso, fui por la fibra óptica del Pacífico. Y allí entré a un proveedor de servicio, que es uno de los que mantiene un servidor raíz, que yo dije que, aparte de mantener el servidor raíz, es un carrier importante, es [inaudible]. Y de allí me llevó directamente hasta Francia, y llegue a le fígaro.

¿Alguna pregunta? Adelante Terri, por favor.

Esa es la forma en cómo navegamos por internet, y cómo previamente a eso se resuelven los nombres de dominio. Adelante, Terri.

Adelante, Carlos.

CARLOS ÁLVAREZ: Gracias Alberto.

¿Qué hacemos nosotros en el departamento?

Un paréntesis muy cortó. Alberto mencionó la existencia de los revendedores de dominios. Y existen, además de los revendedores, las empresas que venden los servicios de privacidad, o de proxy, no sé cuál es la mejor forma de traducir la palabra proxy. Son empresas que le permiten, a las personas, registrar dominios, utilizando la información de contacto de terceros. Incluso sin incluir su propio nombre.

Entonces, si yo registro carlos.com, en lugar de que, en la información de registros de dominio, figure que el dominio fue registrado por Carlos Álvarez, va a aparecer que fue registrado por servicios de privacidad limitada, con la dirección de esa empresa, y el teléfono de esa empresa, y el email de esa empresa, en vez de mi propia información.

Eso es bueno, tiene algunos beneficios obviamente, tiene unos puntos en contra. Pero el punto que queríamos hablar al respecto de los revendedores, es que mientras que existen algunos revendedores, que son empresas éticas, profesionales, serias, existen otros que están por fuera de nuestro alcance, que son un poco más complicado, que representan un cierto reto, por decirlo de alguna manera.

Muchos registradores de ICANN operan revendedores, a través de los que ofrecen al público el registro de dominio. No quiero hablar de venta de dominios, porque sobre los dominios no existe un derecho de propiedad. Los dominios son recursos de red, y como tal, no existe una propiedad, como yo puedo tener un derecho de propiedad sobre mi computador, o sobre mi vehículo, o sobre mi casa.

Los dominios, como decía, son recursos de red, por eso prefiero evitar decir que son vendidos, son registrados. El registro de dominio implica precisamente eso. Se incluye una línea con información sobre el dominio, y el registrante, y los servidores que se van a asociar con sus direcciones IP al nombre de dominio. Y de ahí queda el dominio registrado, básicamente.

Respecto de los revendedores, mencionaba que hay algunos registradores que operan directamente sus revendedores. Esos registradores deben cumplir unas obligaciones contractuales frente a ICANN. Tiene que garantizar que los revendedores cumplan con su contrato. Existe un contrato entre el registrador y el revendedor, y lo tienen que cumplir. En esa medida, los revendedores que son operados por registradores son, quiero decir un poco más confiable, pero no quiero ser la generalización, una generalización injusta, porque pueden existir revendedores que no sean operados por registradores, que sean empresas responsables y serias.

> Entonces, el punto aquí es que, si ustedes van a registrar el nombre de dominio, hagan su tarea completa. Estudien la reputación del registrador, estudien la reputación del revendedor, a través de quien lo van a registrar. Entiendan si el dominio lo van a registrar a través de un revendedor, o directamente a través de un registrador. Si van a hacer uso de servicios de privacidad, al momento de registro. Busquen, en

internet, comentarios de los usuarios acerca de los registradores o revendedores que ustedes están pensando. No se guíen únicamente por el precio. Definitivamente no. Hagan su tarea, para evitar después dolores de cabeza, que pueden pasar, que ciertamente pueden ocurrir.

A muy grandes rasgos, tres áreas, tal vez no son las únicas, pero son las más relevantes, en las que nosotros trabajamos. Primero analytics. ¿En qué consiste?, analizamos grandes cantidades de información de registros de nombre de dominio, y encontramos en ellas, comunalidades, o patrones, que pueden indicar casos de abuso.

Hace unos meses, terminamos un piloto. Estudiamos toda la información de registro de todos los dominios registrados por un sector de industria, acá en Estados Unidos. Encontramos conclusiones preocupantes, encontramos otras conclusiones que fueron muy buenas. Y toda la información la compartimos con ese sector de industria.

Lo hicimos de una manera privada, en confianza con ellos, entendiendo que algunas de las conclusiones no pueden ser hechas públicas, porque ponen a todas esas empresas en riesgo de ser atacadas. Entonces, les haríamos un mal favor si publicáramos esas conclusiones. Obviamente eso no se va a hacer. Pero ese sector de industria recibió muy bien la información, y las empresas tuvieron la oportunidad de felicitarse, respecto de las conclusiones que llegamos, que estaban muy bien, y de hacer los ajustes necesarios respecto de las demás conclusiones.

Ahora estamos en otro proyecto que es muy interesante. El anti-phishing working group, que es un grupo de trabajo contra el phishing, es un grupo sin ánimo de lucro. No quiero usar la palabra asociación, porque no es una asociación, es otra cosa. Es una organización sin

ánimo de grupo, que reúne empresas que se dedican a luchar contra el phishing.

Ahora están extendiendo un poco su alcance a malware también, y botnets. Tiene un servicio, que se llama e-crime, y consiste, básicamente, en que recibe flujos de información respecto a dominios que han sido detectado como siendo utilizados para campañas de phishing, incluso malware. Se analiza la información de registro de los dominios, y se comparte con empresas y registradores, para que tomen medidas y puedan protegerse los unos, y los registradores puedan bloquear nuevos registros, suspender dominios maliciosos, etcétera.

Eso tiene que ver con analytics.

En cuanto a construcción de capacidades, que es el segundo ítem, ICANN no opera directamente infraestructura de internet, salvo el servidor L root, y salvo los sistemas de administración que utiliza IANA. IANA es la autoridad de asignación de números de internet. La función de IANA es crítica para el funcionamiento de todo el sistema de nombres de dominio. Crítica, en sentido de que es el managment que está detrás, y que nadie ve, y que nadie debe ver, en el sentido en que, si nadie sabe que IANA existe, es porque funciona, porque las cosas no se han roto, porque no hay interrupciones.

En el momento en que algo funcione mal, y la gente se pregunte "¿Pero quién cometió un error? ¿Por qué no está respondiendo?", van a empezar a llegar "Ah, fue IANA. IANA cometió un error, los servidores de IANA se cayeron, por eso no está funcionando". A la gente le interesa que las cosas funcionen bien. Entonces, digamos que, es un jugador que está tras bambalinas, operando todo.

Pero, aparte de esos servidores que utiliza IANA, y del servidor L root, nosotros no operamos infraestructura de internet. Por eso, en cuanto a creación de capacidades, lo que hacemos es proveer entrenamiento. Entrenamos unidades cibernéticas de agencias de policía en todo el mundo. Entrenamos a lo

Y literalmente es en todo el mundo. Puede haber semanas, o meses mejor, en las que nuestro equipo esté recabando cinco continentes, y cubramos veinte países, fácilmente. Y cada mes es así, siempre estamos afuera. Entre más entrenamientos podamos proveer, tanto mejor. Entre más podamos difundir los temas que tengan que ver con el funcionamiento del DNS, sobre todo cómo identificar, investigar, detectar, mitigar, contener amenazas en internet, que tengan que ver con identificadores únicos, es decir, dominios y direcciones IP, tanto mejor.

El último ítem, que en inglés lo llamamos trust based collaboration, la traducción al español es medio floja, a mí no me convence, pero es algo así como colaboración basada en la confianza. En español no dice tanto como en inglés. Quiere decir que participamos en grupos de la comunidad de seguridad operacional. Que sea seguridad operacional quiere decir que son las empresas, y son las personas, que están en capacidad de responder frente a amenazas actuales, que pueden afectar a los usuarios, que pueden implicar riesgos serios contra el DNS, que pueden implicar suspensiones de los servicios de resolución del DNS.

Y si el DNS deja de resolver, deja de funcionar. Va a haber regiones del mundo que se van a quedar sin internet, simple y sencillamente. Van a

estar los cables, van a estar los servidores prendidos, pero si yo voy a buscar www.icann.org, no voy a tener respuesta, mi computadora no va a saber a dónde ir para encontrar el contenido del website a donde quiero ir.

En esos grupos, nuestra labor consiste en, básicamente, monitorear la información de inteligencia que es compartida. En términos burdos, mantenemos un ojito para ver qué está pasando. Y cuando vemos que hay amenazas que pueden siquiera, lejanamente, representar un riesgo para el DNS, entramos en acción. Y nuestra acción consiste en facilitar. Nosotros no operamos la infraestructura, no, por eso le ayudamos a la comunidad a enfrentar los riesgos y las amenazas. En términos muy resumidos, creo que eso es lo que hacemos.

Silvia, creo que podemos seguir adelante con preguntas, si alguien las tiene.

SILVIA VIVANCO: Muchas gracias, Carlos. Silvia Vivanco.

Si han terminado las presentaciones, entonces daría paso a las preguntas y respuestas.

Veo algunas personas ahí escribiendo, pero voy a empezar con la primera pregunta, hace un rato, de Sylvia Herlein a Carlos. "¿Cuál sería la función para recordar y guardar nuestro numero MAC? ¿Si nos roban un dispositivo, tenemos que averiguar cuál era nuestro número MAC?"

CARLOS ÁLVAREZ: No, en realidad, el numero MAC, la verdad, es irrelevante para el usuario. Es un número que se utiliza para propósito de enrutamiento. Es para que, en la red interna, el router y las demás máquinas, sepan como encontrar tu dispositivo.

Pero a ti, como persona, no te interesa necesariamente la dirección MAC de ese aparato. Para efectos probatorios, tal vez. Si te roban el teléfono celular, y detienen al ladrón, y resulta que el ladrón tiene tres teléfonos que son exactamente iguales, y los tres teléfonos están reseteados, es decir, que los dejó como si acabaran de salir de la fábrica, si tú tuviste la sagacidad, si quieres decirlo así, de anotar la dirección MAC de tu teléfono antes del robo, y puedes encontrar que uno de esos tres teléfonos tiene ese MAC, pues ya sabes cuál es el tuyo.

Pero eso es todo. No creo que tenga mayor beneficio para el usuario guardar, o aprenderse de memoria, la dirección MAC.

SILVIA VIVANCO: Okey, muchas gracias, Carlos. Es Silvia Vivanco de nuevo.

Tengo otra pregunta sobre los nombres de dominio, de Aida Noblia. Tú mencionaste que no había derecho de propiedad, ella pregunta "¿Sería un derecho de uso?".

Adelante, Carlos.

CARLOS ÁLVAREZ: Voy a esquivar tu pregunta diciendo que en términos técnicos, es simplemente un registro.

En una red, digamos que si se puede entender que recibes un derecho de uso cuando en una red te es asignada la asignación de un recurso, pero prefiero simplemente en esos términos. Cuando tú registras un dominio, te conviertes en el administrador de ese recurso de red por el tiempo durante el que el registro sea válido, eso es todo. ¿Cómo lo puedes usar?, como el dueño de la red te permita.

Eso en términos de internet, ¿Cómo se traduce? Hay muchas cosas que puedes hacer con un nombre de dominio, no solamente poner un sitio web, email, ftp. Una cantidad de aspectos de seguridad puedes manejar también con la información del registro, puedes poner criptografía en el DNS. En fin, eso te lo permite el DNS, en la medida en que tú eres el registrante. Es decir, la persona que figura en la línea de registro, que puede administrar ese recurso de red.

Más que un derecho de uso, es la administración. Te concede la administración del recurso de red.

SILVIA VIVANCO: Muchas gracias, Carlos.

Acá veo un comentario de Aida Nobila. Dice "'ese dominio te da derecho de administrarlo durante un tiempo, entonces".

Luego tengo una pregunta de Nascimento Falleiros, dice "Si es técnicamente un registro, ¿cómo pensar en cuestiones de patentes de marcas? ¿Cuáles son los desafíos para el mercado de América Latina?".

CARLOS ÁLVAREZ: Alberto, yo no sé si tú quieres coger esa pregunta.

ALBERTO SOTO: Es una muy buena pregunta.

El caso es que cuando hablamos de dominios de alto nivel, toda esa política está perfectamente clara dentro de ICANN. Cuando hablamos de dominio que representa a una empresa, o a una persona, a una organización, el tema netamente diferente. Hay controversias, hay litigios. Hay una entidad que se encarga de litigios, pero si yo la elijo, normalmente no nos encontramos con mucha legislación respecto de nombres de dominios.

Si está claro, en muchos países, por ejemplo en dominios de alto nivel, quién puede acceder a un .org o a un [inaudible]. En Argentina, solamente puede acceder una entidad sin fines de lucro, y que esté registrada en el registro de sociedades correspondiente. Y el trámite puede realizarse por internet.

En ese tipo de cosas de dominio de alto nivel, no hay demasiados problemas. Hay pocos, pero no tantos. Respecto de los nombres de dominios, hay toda una discusión si debo considerarlo una marca, o no.

Voy a mencionar algo, adidas.com, qué pasa si hay alguien que lo reservó primero. Primero al llegar, primero en el derecho. Todavía hay controversias muy grandes sobre esto. Inclusive hubo un apellido, recuerdo un nombre de dominio, alguien que fabricaba zapatos en Argentina, y un locutor español. Y finalmente la OMPI, que es la Organización Mundial de Propiedad Intelectual, le dio el dominio al locutor español porque era más popular el fabricante de zapatos argentino.

Por supuesto que estoy en total desacuerdo con eso. Para mí, en ese caso, es el primero en llegar, el primero en el derecho.

Todavía hay cosas muy conflictivas respecto de, si yo tengo patentada una marca, o registrada una marca, me da derecho o no. Depende de cada país, porque eso lo maneja cada país.

Adelante.

CARLOS ÁLVARES: Quiero complementar un poquito lo que mencionó Alberto.

En el mundo de ICANN nada más, existe la política de la uniform domain name resolution policy, que es la UDRP, y existe también en el mundo de los neo gTLDs, que son los nuevos dominios, una política que se llama URS, Uniform Rapid Suspension system, el sistema uniforme de suspensión rápida.

Básicamente, la UDRP le permite a los titulares de derechos de marketing iniciar unos procesos administrativos sencillos, rápidos, y de un costo relativamente bajo, cuando quiera que alguien registre sus marcas, o variaciones de sus marcas, bajo las siguientes condiciones que voy a mencionar acá. Lo estoy leyendo literalmente de la política. Que el nombre de dominio sea idéntico o similarmente confundible, que se pueda confundir con una marca, respecto de quien inicia el UDRP, el procedimiento, tiene derecho. Que quien registró ese dominio no tenga derechos, o no tenga un legítimo interés respecto del dominio. O que el dominio haya sido registrado, o esté siendo usado de mala fe.

La cantidad de casos que se ve, en el mundo del spam, respecto de dominios registrados únicamente con fines de enviar spam, y si recuerdan, el spam no es solamente el envío incómodo, para los usuario, de toneladas y toneladas de mensajes irrelevantes. El spam es un medio para un fin. El fin es infectar máquinas con virus, robar credenciales de acceso a cuentas de bancos. El fin es reclutar computadores para que hagan parte de botnets, y muchas veces, todas esas actividades de orden secundario, son facilitadas por el registro [inaudible] de marcas de terceros.

Entonces, quería añadir un poquito eso. Gracias.

ALBERTO SOTO: Alberto Soto nuevamente.

Ya que Carlos, hace un rato, mencionó algo, no quiero dejar pasar, no iba a llegar a ese nivel, pero no quiero dejar pasar. Carlos dijo que teníamos que tener cuidado, o que miremos un poco a ver el registrador, y no nos guiemos por los pesos, o lo que cueste. En realidad, hay registradores de confianza, y hay, cómo diría, si yo hago mi reserva, a mi nombre, no hay ningún problema. Ahora, si yo voy a un proveedor de servicios que dice "bueno, yo le alojo la página web", "bueno, hágame todo". Le hace todo, le reserva el dominio a su nombre, no a nombre de quien está con la página web.

Tengo cientos de casos de esos, que después quisieron recuperar. Se pelearon con el proveedor de servicio, y no podían recuperar su dominio. O lo reservó el técnico que generó la página web. Hay varios

escalones donde el usuario individual puede llegar a hacer su reserva de nombre de dominio.

Yo aconsejo que hagan todos los trámites ustedes o, aparte de tener la seguridad del registrador, ante quien quieren registrar el nombre de dominio, que lo hagan personalmente y obtengan, cuando se vayan, el nombre de dominio a su nombre, no a nombre del programador, o a nombre del proveedor de servicios de internet.

Nada más.

SILVIA VIVANCO: Muchas gracias, Alberto. Es Silvia Vivanco otra vez.

No veo otras preguntas. Quería dar una oportunidad a que levanten la mano. ¿Tenemos algunas otras preguntas? Me parece que no.

Alberto.

ALBERTO SOTO: No es una pregunta, pero justamente ayer en el webinar estuvimos con Steve Conte, y hablamos del problema de seguridad de la información que existe en internet. El mayor problema que tenemos, para aquellos que no estuvieron en el webinar de ayer, es la falta de legislación que hay en nuestra región, en los países de nuestra región.

Esas direcciones IP que son asignadas a nosotros, una dirección IP que es dinámica, que cada vez que ingreso puede ser diferente, o no, a veces es la misma, eso debería quedar registrado en un lugar en el proveedor de servicios. Pero no hay una ley que obligue a mantener

registrada esa dirección por un tiempo determinado. Entonces, cuando se investigue un delito, y se trate de ir a ver ese registro, es altamente probable que no lo encontremos porque no hay una ley que le diga al proveedor de servicios que guarde, por determinado tiempo, esa información, que no es un dato de contenido, sino que es un dato denominado de tráfico.

En Europa, la mayoría de los países, los proveedores de servicios lo tienen por dos años. Y está bien porque, normalmente por el tipo de delito que se comete, puede llegar la prescripción dentro de dos años, y ya no es necesario.

Nada más que eso. Gracias.

SILVIA VIVANCO: Muchas gracias, Alberto. No veo otras preguntas en el Adobe Connect. Sin embargo, tengo yo una pregunta, si me permite Carlos Álvarez, de mi parte.

Carlos, mencionaste que hay una relación de ICANN con agencias policiales cibernéticas, ¿En qué consiste esa relación?, si podrías darnos un ejemplo, por favor.

CARLOS ÁLVAREZ: Primero, como indiqué hace un momento, nosotros entrenamos agencias de policía virtualmente en todos los continentes. Estamos haciendo entrenamientos en América Latina, en Europa, acá en Estados Unidos, en Asia Pacifico, en todos los continentes estamos entrenando unidades ciber.

Una cosa interesante que hemos encontrado es, incluso las unidades cibernéticas que tienen experiencia en estos casos, encuentran que este tema es una subespecialización, dentro de la especialización de delitos informáticos, es algo muy específico. Las investigaciones de delitos que se enfocan hacia la identificación de personas, y de modos operandis que hacen uso o abuso de recursos del DNS, es algo muy específico, es algo muy particular.

Por eso, recientemente hemos estado entrenando fiscales del Departamento de Justicia, el FBI, DEA, [inaudible], Interpol. En América Latina estamos organizando, para la reunión de Buenos Aires, un entrenamiento bien interesante con la policía metropolitana de Buenos Aires, esperamos que esté la federal también, que estén fiscales de la unidad de cibernética. Vamos a estar en Chile en Agosto, en Julio vamos a estar en Colombia, proveyendo entrenamiento también, por mencionar cosas específicas de la región. El año pasado estuvimos en Bolivia, en Diciembre, haciendo un entrenamiento en línea, y estoy hablando de lo mío solamente, de lo que a mí me corresponde.

Pobremente a finales de este mes, o en algún momento en Mayo, voy a estar dando un entrenamiento a una unidad de policía de Zambia, en África.

Entonces, por un lado es el entrenamiento, por el otro, siempre tenemos las puertas abiertas para cuando hay unidades de policía que están adelantando alguna investigación y tienen un bloqueo, quiero decir cuando no saben cómo encontrar más información. Nosotros no les damos la información porque no es algo que nos corresponde, nosotros no somos policías, ICANN no es una agencia de policía, no es

una agencia de investigación. Pero les explicamos, al igual que a quienes atienden a nuestros entrenamientos, cómo pueden hacer ellos mismos para encontrar la información que necesitan. Si necesitan encontrar información de un archivo de zonas, si necesitan encontrar información acerca de un registrante de una serie de dominios, lo que sea, les explicamos. Nos tomamos el tiempo, nos sentamos con ellos, viajamos y nos reunimos con ellos, con sus equipos, de manera que sus investigaciones puedan ser completadas exitosamente.

Y por otro lado, hay formas de malware que utilizan algoritmos para la generación automatizada de dominios, ejemplos recientes, crypto-locker, y otro virus que se llama game over zeus. Los delincuentes incluyen, dentro del código malicioso, algoritmos que son sofisticados, que le permiten a las máquinas infectadas, a la botnet, registrar de forma automática, dominios con ciertas características. Esos dominios se reconocen porque suelen tener la misma cantidad de caracteres alfa o alfanuméricos. Son fácilmente reconocibles cuando son generados de forma automatizada.

Cuando, como decimos entre chiste y charlas, cuando los good guys, o los que estamos del lado bueno de la fuerza, cuando la gente en la comunidad de seguridad logra descifrar esos algoritmos de generación automatizada de dominios, se puede prever fácilmente cuales son los dominios que se van a registrar, para esa botnet, mañana, al día siguiente, la próxima semana, en un mes, en siete años, en diez años, porque son fórmulas matemáticas. Y cuando se encuentra cual es la lista de dominios que la botnet va a utilizar para su comando y control, pues ya se está un paso adelante de los criminales y se puede tumbar la mayor parte de la infraestructura de la botnet, y se deja un pedacito

chiquito para analizar el tráfico de las máquinas comprometidas para ver qué más se encuentra.

Y eso no lo hacemos nosotros directamente, lo hacen las agencias de policía. Pero cuando logran descifrar esos algoritmos, requieren el apoyo de ICANN para que los registros bloqueen o registren anticipadamente todos esos dominios, que serían registrados adelante, por los algoritmos, vía código malicioso.

En términos generales, eso es, Silvia, creo yo.

SILVIA VIVANCO: Muchas gracias, muchas gracias, Carlos.

Si, esto también me parece que responde la pregunta de Víctor Fernández, que escribe en inglés, "si hay investigadores, en esta evolución del DNS, que faciliten la identificación de un usuario, en un crime cibernético, por ejemplo".

CARLOS ÁLVAREZ: Definitivamente, claro que sí.

Hay muchos investigadores, muy buenos, en muchos países, que logran encontrar tanta información, y estoy hablando de personas éticas, de personas que se preocupan por defender a los usuarios. Que trabajan incluso de forma voluntaria en estos temas. Que tienen los niveles de preparación y conocimiento matemático, y de programación altísimos, y que donan su tiempo, o trabajan a cambio de un sueldo, como hacemos muchos, para proteger a la gente. Y claro, estos investigadores existen,

y están ahí desde hace un tiempo, y logran cosas que a veces, realmente, lo dejan a uno con la boca abierta.

SILVIA VIVANCO: Muy bien, Carlos, muchas gracias por ésta explicación bastante exhaustiva.

Y bueno, ya estamos terminando este webinar. Le quiero dar gracias, otra vez, a Alberto Soto, a Carlos Álvarez, por su exponencial, ricas en contenido, que nos han ilustrado muchísimo, y a mi colega Rodrigo Saucedo por la organización. Y por supuesto, al staff de At-Large, Terri por su apoyo, y a todos ustedes que participaron activamente de este webinar. Muchas gracias.

Les digo que tenemos ya las presentaciones subidas en la página wiki, en un wiki page. Las grabaciones estarán listas, me avisan que en cinco días, y las transcripciones también van a estar listas en los tres idiomas, en inglés, en español y en portugués, también en una semana en la página wiki de este webinar, para que lo puedan revisar y puedan repasar estos conocimientos que hemos adquirido hoy día.

Bueno, con esto me despido. Buenas noches a todos mis amigos en Latinoamérica, un abrazo fraterno. Gracias.

ALBERTO SOTO: Gracias, Alberto Soto, gracias a todos, gracias Carlos. Un abrazo grande para todos. Gracias.

CARLOS ÁLVAREZ: Igualmente, Alberto. Gracias, Silvia. Hasta luego todos.

SILVIA VIVANCO: Adios.

[FIN DE LA TRANSCRIPCIÓN]